ENHANCING SECURITY IN HOME AUTOMATION SYSTEM

FIELD OF THE INVENTION

[0001] The present invention relates generally to smart environments. In particular, this pre-set invention relates to security in automation systems and methods that are configured to automatically and/or remotely control products, devices and appliances in a house or other residential or commercial building.

BACKGROUND OF THE INVENTION

[0002] Home automation involves controlling various devices or systems that can be present in homes. Home automation technologies can allow for local and/or remote control of home automation devices. Typically, home automation may include remote and centralized control of lighting, HVAC (heating, ventilation and air conditioning), appliances, security locks of gates and doors and other systems, to provide improved convenience, comfort, energy efficiency and security. The popularity of home automation has been increasing greatly in recent years due to much higher affordability and simplicity through smart phone and tablet connectivity. The concept of the Internet of Things (IOT) has tied in closely with the popularization of home automation. The Internet of Things (IOT) is the network of physical objects or “things” embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Further, it is also important to support and protect such closed networks and all connected devices, through one or more security standards. The conventional security standards include protection or prevention from theft or damage to the hardware, software and information passing through them. It further includes controlling of physical access to the hardware and protecting against one or more harm which comes through network access, data injection of malicious code which may occur due to the malpractice by users, operators, which are intentional, or accidental, or due to them being tricked into deviating from secure procedures.

[0003] As society advances, households within the society may become increasingly diverse, having varied household norms, procedures, and rules. Unfortunately, because so-called smart devices have traditionally been designed with pre-determined tasks and/or functionalities, uses one or more conventional security methods, comparatively fewer advances have been made regarding using these devices in diverse or evolving households or in the context of diverse or

evolving household norms, procedures, and rules. Accordingly, there is still a need for improved and advanced security in home automation systems, methods, and technologies, to provide confidentiality, integrity and authentication.

SUMMARY OF THE INVENTION

[0004] The present invention provides a security in home automation system and a method of operating thereof. The method includes the steps of: inputting a data in the wearable device of user to connect to a home automation module through the security module, securely transmitting the data to the security module, checking and analyzing the data for an security pattern, identifying the security pattern by comparing the subject data with the stored data and approving and authorizing the user to access home automation module. In an embodiment, every user of home automation system has a profile data, security pattern, configuration data. In another embodiment, the security pattern may be one of or combination of, a gesture, accelerometer, gyro values, pin and password.

[0005] To further clarify advantages and features of the present invention, a more particular description of the invention will be rendered by reference to specific embodiments thereof, which is illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail with the accompanying drawings.

BRIEF DESCRIPTION OF FIGURES

[0006] These and other features, aspects, and advantages of the present invention will become better understood when the following detailed description is read with reference to the accompanying drawings in which like characters represent like parts throughout the drawings, wherein:

[0007] Fig. 1 is a system illustrating a home automation module with a security module in an embodiment of the present invention.

[0008] Fig. 2 illustrates the example scenario in which plurality of smart wearables are connected to the home automation module through the security module.

[0009] Fig. 3A, 3B and 3C illustrates the example combination of connections between the smart wearable devices, security module and the home automation module.

[0010] Fig. 4 is an example flowchart illustrating the steps involved in authenticating/authorizing the user for home automation module by the security module in an embodiment of the present invention.

[0011] Figure 5A illustrates an example authorization pattern performed through hand 500 in an embodiment of the present invention.

[0012] Figure 5B, 5C and 5D illustrates the five different positions (520, 530, 540, 530 and 520) of hand 500 in an embodiment of the present invention.

[0013] Figure 6A and 6B illustrates an example configuration data stored in the security module.

[0014] Further, skilled artisans will appreciate that elements in the drawings are illustrated for simplicity and may not have been necessarily been drawn to scale. For example, the flow charts illustrate the method in terms of the most prominent steps involved to help to improve understanding of aspects of the present invention. Furthermore, in terms of the construction of the device, one or more components of the device may have been represented in the drawings by conventional symbols, and the drawings may show only those specific details that are pertinent to understanding the embodiments of the present invention so as not to obscure the drawings with details that will be readily apparent to those of ordinary skill in the art having benefit of the description herein.

DETAILED DESCRIPTION OF THE PREFERRED EXAMPLES

[0015] Fig. 1 is a system diagram 100 of network of devices in embodiment of the present invention. The system comprises, smart wearable device 102, a mobile device 104, a home automation module 106, an application server 110, a database 112. The home automation module 106 further comprises a security module 108. The smart wearable device 102 and mobile device 104 are directly connected to the home automation module 106 through the security module 108. In an embodiment, the security module 108 is an internal component of home automation module 106 or a standalone module externally connected with the home automation module 106. The security module 108 is used to provide set of one or more policies, practices which are to be adopted to provide access to the authorized user and to prevent and prudently monitor unauthorized access, misuse or modification of data in the home automation module 106. In one embodiment, the security module 108 is a series of one or more integrated modules connected in the same runtime environment. The security module 108 is capable of authenticating the user (of the smart wearable device 102 or mobile device 104) for home automation module 106, through one or more pattern of actions performed by the first user through the subject smart wearable device 102. In other words, the security module 108 manages the user, and organizes user profiles, user actions, user activities to streamline the accessibility for the home automation module 106.

[0016] The security module 108 receives one or more inputs from the user's smart wearable device 102 and mobile device 104. The security module 108 further extends permission/access to the user for home automation module 106, only when the user is successfully validated by one or more authorization methods. While configuring the security for home automation module 106, the user may enter a pin /setup an action/pattern (for example, gesture, accelerometer/gyro values, pin, password, iris data, finger print etc), in the security module 108 and to access the home automation module 106. The application server 110 and database 112 are connected to the home automation module 106 to centrally process the queries, of one or more users, which are received from one or more smart wearable devices 102 and mobile devices 104. In an embodiment, the database 112 is a centralized repository, wherein all policies, procedures, profiles, activities and any data with respect to home automation module 106 and security module 108 kept in an organized manner and securely stored. In an embodiment, the security module 108 receives user query to access home automation module 106, when the user is in vicinity of his home. In another embodiment, the user may remotely control home automation module 106 only when such access is authorized by the security module 108, and wherein, security module 108 provide such access to one or more selected devices of the user.

[0017] In an embodiment, the smart wearable device 102 is also capable of detecting any actions/patterns/gestures performed by the user, through one or more sensors, configured thereon, which forms the authorization pattern (a security pattern) to access the home automation module 106. In another embodiment, the one or more actions/patterns/gestures may be sequentially performed, one after the other, by the user to complete one authorization pattern. In other words, the authorization pattern to access the home automation module 106 may be one action or series of actions, that are performed in a smart wearable device 102. When such actions are performed by the user, the sensors units configured in smart wearable device 102 is allowed to capture and record the such one or more series of action, sequentially and consider them as an authorization pattern or a security pattern.

[0018] The security module 108 is configured to allow only such user, who performs pre-configured actions/pattern through the one or more connected smart wearable device 102. The pattern is not device specific, the user can use any smart wearable device 102 and perform his/her authorization pattern to access the home automation module 106. The actions, which are captured by the smart wearable device 102 are stored as a 'pattern' and transmitted (as an encrypted content) to the security module 108 through one or more communication methods or standards, that include, but not limited to, Bluetooth, WiFi, NFC.

[0019] In an embodiment, the security module 108 enables the home automation module 106 only when user is identified and authorized by the security module 108. Once, the user is authenticated, the home automation module 106 will allow commands/inputs from the subject smart wearable device 102.

[0020] In one example, when the smart wearable device 102 is worn by the user (in the vicinity of security module of home automation module/hub), the smart wearable device 102 prompts the user to perform the actions in order to authorize the user. In another embodiment, the smart wearable device need not be in the vicinity of security module, and the communication between the smart wearable device and security module happens through one or more medium and long-range communication standards, which include not limited to, cellular networks, LoRaWAN. The security module processes the data from the user and authorize the user only when the input data from the user is matching with the stored data. Further, after authorization, the security module 108 creates a session and unlocks the features, configured for the subject user, and the user's smart wearable device 102 provide one or more options and accessibility for the user to interact with the home automation module 106. In one example, the user any time during the ongoing session, can pause the session for 10-15 minutes, by tapping the smart wearable device 102 or performing an action in the mobile device 104 and later resume the session. Also, the user can terminate the session any time. In another embodiment, when the session is inactive for more than 10 minutes, the security module 108 automatically terminates the subject session, and request the user to perform authorization pattern to confirm and re-authorize the access to the home automation module 106.

[0021] In an embodiment, the security module 108 scan for devices either new or already connected devices and further particularly identifies smart wearable devices which are in the range and vicinity. If it is a new device, and subject user requests the access for home automation module 106, by manually initiating a request in mobile device 104 (through a mobile application) or through tapping the smart wearable device, twice (for example), then the security module 108 initiates a configuration procedure and setup the user to access home automation module. During the configuration stage, the security module 108 requests the user to set an authorization pattern/action to authorize him/her for the home automation module 106. The subject authorization pattern/action are stored in the security module 108 as well as processed by the application server 110 and eventually stored in the database 112 of the system. Further, while configuring new devices, the user may manually enter one or more particulars of smart wearable device 102. The particulars may include user and device details, for example, name, age, type of smart wearable device (for example, smart watch, analog watch, band or

any IoT device), with their unique ID etc. In an embodiment, the security module and home automation module may have a unique ID, or passcode, which is only known to the user (who had purchased the modules). The user details, device details (smart wearable device, mobile device, security module, home automation module) along with the authorization pattern are processed by the application server 110, and stored as 'user configuration data' in the profile of the user in database 112. Further, a copy of user configuration data is stored in the memory of security module 108. In an embodiment, the security module 108 may store up to 10 user configuration data. During configuration, the user can create a group of users who need to access the home automation module. Upon such group creation, an invitation request is immediately shared with the other users to provide their smart wearable device details, mobile device details, profile details, and to configure their authorization pattern for the subject home automation module. In another embodiment, the invitation request can only be created by a super user. In yet another embodiment, the super user is a normal user, who has advanced authorization access to both security module and home automation module.

[0022] In another example, the user can configure one or more authorization pattern/action to access home automation module 106. The example authorization pattern/action may be 'two claps' followed by 'two punches'. This action of the user is sequentially captured by the smart wearable device 102 and the same is being registered by the security module, along with the details of subject smart wearable device 102.

[0023] In yet another embodiment, the security module 108 may suggest one or more authorization patterns for the user and user can choose any one or more such patterns which may be sequential in nature and subsequently register with the security module 108. In another embodiment, the action may be one of entering a code (password, or pin) or finger print authorization on the smart wearable device 102. The user can configure plurality of patterns/actions (through smart wearable) in the security module and to access the home automation module. In another embodiment, a smart wearable can recognize one or more authorization patterns/actions of the user. In yet another embodiment, the smart wearable is specific to one action/pattern.

[0024] Further, the security module 108 can only be accessed by a super user, who configures and monitors home automation module 106 and provide access to one or more users. The security module 108 may limit the number of users to access the home automation module 106 or super user can configure the total number of users for a home automation module 106.

[0025] Further, the security module 108 provide access to all components in home automation module 106. The accessibility can be provided to control and monitor door/window, kitchen,

lighting, one or more rooms, electricity, water flow and all other components which are part of home automation module 106.

[0026] In an example, the smart wearable device 102 is a watch (analog), which is used to capture user actions (through pressing the crown, like one press, two press etc) or through one or more buttons, the security module 108 appropriately identifies the user action through the connected watch. The pattern for analog watch may be different from another smart wearable device and have a different configuration procedure. In another example, the smart wearable device 102 is a smart watch/ band or any apparel, having a display screen, which is used to capture user actions (through tapping the screen, or gesture actions, patterns etc), the security module 108 appropriately identifies the user action through the connected smart watch/band or apparel.

[0027] In an embodiment, the security module 108 authenticates the user every time he wears the smart wearable device 102, and authorize the user, to send the instructions for the home automation module 106. In another embodiment, when the smart wearable device 102 is removed by the user and the authorization is automatically cleared by the security module 108. Further, the smart wearable device 102 may have a proximity sensor, usually at the back, to particularly detect the device is being removed from hand (of the user who was wearing it), hence the authorization is cleared, and nobody shall be able to access the home automation module 106. If in case, when the smart wearable device 102 is forcefully removed from hand, then also the authorization is cleared immediately, through the readings from accelerometer sensor.

[0028] In an embodiment, the smart wearable device 102 may be worn by two people, then based on their action/ pattern, the security module 108 identifies the user and grant authorization to the home automation module 106. In another embodiment, each IoT component in home may be configured with an authorization pattern, which is validated by the security module 108 of home automation module 106. When the security module 108 receives the accurate pattern for the selected IoT component, only then the home automation module 106 shall grant permission to selected IoT component, otherwise access is denied, for example, safety locker.

[0029] Figure 2 illustrates the example scenario in which plurality of smart wearables are connected to the home automation module through the security module. Each of the smart wearable device 102_2, 102_4, 102_6...102_n is paired with the home automation module 106 and the security module 108 of home automation module 106 is capable of identifying the smart wearable device 102_2, 102_4, 102_6...102_n in real-time and also capable of switching between user

configuration settings. Each smart wearable device 102 is authenticated by the security module 108 and the security module is capable of authorizing the smart wearable devices 102 for home automation module 106.

[0030] Figure 3A, 3B and 3C illustrates the example combination of connections between the smart wearable devices, security module and the home automation module.

[0031] In an embodiment, the security module 108 (of home automation module 106) stores profiles of user. The profiles of user further comprise, Unique identification number (UIN), device name, wearable type, configurations, authorization patterns/values, commands/instructions to be performed for scheduled activities, total active duration of profile, list of all IoT components connected with home automation module, accessible list of IoT components, threshold values for each IoT component, condition of each IoT component (active/idle) etc. The security module 108 provide access to the home automation module 106 by authenticating the user with authorization patterns.

[0032] Figure 3A illustrate combination of one smart wearable device 102_2 paired with the home automation module 106 and connected through the security module 108. Figure 3B illustrate combination of two smart wearable devices 102_2 and 102_4 paired with the home automation module 106 through the security module 108. Figure 3C illustrate combination of three smart wearable devices 102_2, 102_4, and 102_6 paired with the home automation module 106 the security module 108. The home automation module 106 is configured to receive commands from smart wearable devices 102_2, 102_4, 102_6.

[0033] In an embodiment, a single user can have multiple profiles (configuration settings for connected IoT components) in the home automation module. In another embodiment, the user may select a profile (from the list of profiles) to be exhibited by the home automation module. In another embodiment, each user may have a default profile. The profiles are specific in nature and vary between user to user. The home automation module 106 is pre-programmed to accept and execute the instructions based on the profile data.

[0034] Figure 4 is an example flowchart illustrating the steps involved in authenticating/authorizing the user for home automation module by the security module in an embodiment of the present invention. The method 400 includes the step 410 of inputting a data in the wearable device to connect to a home automation module through the security module. The input data is appropriately captured by the wearable device and the subject data is being securely transmitted to the security module in step 420. In an embodiment, the data is encrypted by one or more encryption standards. Further, in step 430, the security module receives the data from the wearable. The security module may use the one or more decryption standards to

decrypt the encrypted data. In step 440, the method 400 performs a check whether the data received is an authorization pattern. In an exemplary implementation, the security module may use one or more matching technique to identify the subject data is an authorization pattern. In an embodiment, the authorization pattern may have a unique ID and user ID, through which, the security module identifies such pattern from the wearable devices. When, the security module identifies the received data is an authorization pattern then the control is transferred to step 450, otherwise, the control is transferred to step 460. In step 450, the security module extracts the pattern into first values or first set of values. In one example, the data having authorization pattern is segmented into various parameters, such as user name, device type, device id, authorization type etc. During configuration of home automation module through the security module, a unique id is configured for each user. In an implementation, the unique id may be same for all the smart wearable devices belonging to the same user. In step 470, the security module check whether the first values match with the already stored values of subject user. If the values are matching then the user is approved and control is transferred to step 480, otherwise, the control is transferred to step 460. In step 480, the security module authenticates and authorizes the user for home automation module, and provide access to only those components of home automation module, attributing to respective home automation policy. In step 460, the security module requests the user to re-enter the data having authorization pattern.

[0035] Figure 5A illustrates an example authorization pattern performed through hand 500 in an embodiment of the present invention. As shown there, the user is wearing a smart wearable device 510, who performs the authorization pattern, in this case waving a hand sideways. The 'waving hand sideways' authorization pattern is split into 5 partial patterns (at each position of hand). The smart wearable device 510 having one or more sensors, identifies movement of hand which is considered as position of the hand. The smart wearable device captures the data and accommodate them as one single authorization pattern or sequence of authorization pattern. In this example, the smart wearable device identifies first position (520), second position (530), third position (540), fourth position (530) and fifth position (520) of the hand and combines them as 'one single authorization pattern'. Similarly, various other actions are captured by the smart wearable device and such action in the form of data are transmitted to the security module for authorization. Figure 5B, 5C and 5D illustrates the five different positions (520, 530, 540, 530 and 520) of hand 500 in an embodiment of the present invention.

[0036] Figure 6A and 6B illustrates an example configuration data stored in the security module. As shown there, in an embodiment, each user has a profile data, security pattern, configuration data in the home automation system. The profile data may include, name, age,

type of smart wearable device (for example, smart watch, analog watch, band or any IoT device), with their unique ID etc. The security pattern is one of or combination of pin, password, biometric, gesture actions. The user 1 in figure 6A is connected to the security module, wherein, user can enter the authorization pattern only through pattern (gesture) pin and biometric. The security module further receives only those input from the connected smart wearable device, for authorization. The user in figure 6B is connected to the security module, wherein, the user is limited to enter the authorization only through pattern and pin. Further, user enter one or more security patterns to access the home automation module, but however, such user may be accessible to few of the IoT components in home automation module. In an embodiment, the configuration data holds the key list of components that are to be accessed / operated by the user or users, in reference to all IoT components in the home automation module. The user 1 in figure 6A is having a set of authorized IoT components in home automation module. The user 1 can only have access to control 'light 1' (Access: ALL) and 'light 2' (Access: On/Off only), whereas the user does not have access to control 'motor 1' (Access: None). Whereas, the user 2 in figure 6B is also having another set of authorized IoT components in home automation module. The user 2 having access to control 'TV-Remote' (Access: ALL), 'Chimney' (Access: On/Off only), 'Coffee maker' (Access: ALL), 'Lights' (Access: ALL) and and 'Fan & AC' (Access: Yes - Auto cool only). In the similar way, one or more users of the home automation system may have access to one or more IoT components. In yet another embodiment, each of the IoT component may have a separate second level of authorization, which are monitored by security module. The super user may configure the first and second level of authorization. The first level of authorization is the authorization provided to access home automation module, whereas, the second level authorization is device or IoT component specific, which may require additional authorization. Further, the security module may have a list of IoT components which may require additional authorization. In another embodiment, the user can configure a security pattern for those components in the subject list and securely access them, by providing the such action/pattern. For example, a safety locker may have second level of authorization, but in order to access the safety locker, the user must pass the first level of authorization, as configured in security module.

[0037] While various embodiments of the present disclosure have been described above, it should be understood that they have been presented by way of example only, and not limitation. Thus, the breadth and scope of the present disclosure should not be limited by any of the above-discussed embodiments but should be defined only in accordance with the following claims and their equivalents.

Claims

We Claim:

1. A system (100) for authorizing a user to provide access to home automation, said system (100) comprising:

   a smart wearable device (102) configured with one or more motion and biometric sensors, wherein the smart wearable device (102) detects a first set of user actions and biometric parameters of a subject user and to generate a first data comprising the first set of user actions, biometric information, and profile information of the subject user,

   characterized in that:

   a communication network, wherein, the subject first data from the smart wearable device (102) is encrypted and transmitted to a security module (108) through the communication network;

   a home automation module (106) comprising the security module (108), wherein the security module (108) is configured to decrypt and analyze the first data, extract and identify at least one of an authorization type and a usage pattern, validate the extracted data by comparing with a set of multi-modal authorization profiles stored in a database (112) corresponding to the subject user, and grant access to the subject user for a plurality of IoT (Internet of Things) devices configured in the home automation module (106), wherein the home automation module (106) is enabled by the security module (108) only upon successful authentication of the user, based on the combined evaluation of the gesture pattern and biometric information, wherein the security module (108) is configured to generate a dynamic session key based on the user's role and access level, and to manage the subject user by maintaining organized data including user profiles, user actions, user activities, and session states, thereby optimizing accessibility for the home automation module (106), and wherein the smart wearable device (102) is further configured to detect removal from the user's body and to automatically revoke the subject user's authorization in real time.

2. The system as claimed in claim 1, wherein the smart wearable device (102), configured with one or more motion and biometric sensors, is configured to detect a first set of actions comprising a single action, a sequence of actions, or a gesture, while simultaneously capturing at least one of a biometric information.

3. The system as claimed in claim 2, wherein the smart wearable device (102) captures one or more positions and movements of at least one hand of the subject user in real time, and maps the captured data to a gesture pattern which is synchronized with variations in biometric information recorded during the movement.
4. The system as claimed in claim 1, wherein the smart wearable device (102) comprises at least one of a smartwatch, analog watch, wearable band, or any IoT device, including a biometric module configured to detect at least one physiological parameter while the subject user performs a gesture.
5. The system as claimed in claim 4, wherein the authorization pattern in the analog watch is generated by the subject user through pressing one or more crowns, wherein each press is validated by generating a time-stamped hardware token, forming part of the authorization pattern.
6. The system as claimed in claim 1, wherein the smart wearable device (102) is operable in either a sequential or simultaneous manner to generate at least one composite authorization pattern comprising motion data and biometric information.
7. The system as claimed in claim 1, wherein the IoT devices in the home automation module include at least one of light, fan, AC, door, motor, TV, coffee maker, chimney, electrical circuits, and safety lockers.
8. The system as claimed in claim 1, wherein granting access comprises permitting the subject user to interact with at least one IoT device by performing at least one of the following actions of opening, closing, operating, checking status, viewing, or modifying the configuration settings of the respective IoT device.
9. The system as claimed in claim 1, wherein the authorization type includes at least one, or a combination, of PIN, password, gesture pattern, accelerometer and gyroscope values, iris data, and fingerprint data, wherein the authorization pattern comprises security related information used to determine the user's identity and access privileges.
10. A method for storing user information, the method comprising:

inputting and capturing, by a smart wearable device (102), a first set of actions and biometric parameters of a user, and generating a first data set by the smart wearable device (102), wherein the first data includes at least one of the first set of actions, biometric information, device type, device ID, and the name of the user;

encrypting and transmitting the first data, through a communication network, to a security module (108);

processing, by the security module (108), the received first data to extract at least one of an authorization type and pattern, along with the associated biometric information;

authenticating the user by verifying the extracted information with multi-modal authorization profiles; and

storing, in a database (112), the validated data as part of a user profile, including device details, configuration settings, and access rules associated with the security module (108) and the authorized IoT devices within the home automation system.

11. The method as claimed in claim 10, wherein the first set of actions comprises at least one, or a combination, of an authorization type and an authorization pattern.
12. The method as claimed in claim 11, wherein the authorization type includes at least one, or a combination, of PIN, password, gesture pattern, accelerometer and gyroscope values, iris data, and fingerprint data, wherein the authorization pattern comprises security information used to determine the user's identity and level of access.
13. A method for authorizing a user to provide access to a home automation system through a smart wearable device (102), the method comprising:

detecting and preparing, by one or more motion and biometric sensors, a first set of actions performed by a user along with corresponding biometric and user information, wherein the smart wearable device (102) encrypts the resulting first data;

transmitting the encrypted first data to a security module (108), wherein the security module (108) is configured to decrypt and analyze the received first data, and validate the user's identity through combined verification of gesture data and biometric information against reference data stored in a database (112), wherein, upon successful validation, the security module (108) generates a temporary session key and assigns a tiered access scope to selected IoT devices, and wherein the home automation module (106) is enabled only during an active session, and with the session being automatically revoked upon removal of the wearable device or upon expiration of a predefined session timer.

14. The method as claimed in claim 13, wherein the user initiates a session through the smart wearable device (102), and pauses or terminates the session using a biometric gesture.
15. The method as claimed in claim 13, wherein access to IoT devices is restricted based on the user profile, and context based access control rules.